AL:MKP
F.#2017R00050

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

18M 55

IN THE MATTER OF THE SEARCH OF TWO CELLULAR PHONES CURRENTLY LOCATED IN QUEENS, NEW YORK	APPLICATION FOR SEARCH WARRANTS FOR TWO ELECTRONIC DEVICES Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, PAUL TAMBRINO, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of property—two electronic devices, further described in Attachments 1-A and 2-A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachments 1-B and 2-B.

2. I am a Special Agent with Federal Bureau of Investigation, and have been for approximately 22 years. I am currently assigned to the squad tasked with investigating the Gambino and Luchese organized crime families of La Cosa Nostra (the "Gambino crime family" and the "Luchese crime family"). During my tenure with the FBI, I have participated in long-term organized crime investigations, during the course of which I have conducted physical and electronic surveillance, executed search warrants (including on electronic devices), reviewed and

analyzed location data and reviewed and analyzed numerous taped conversations and debriefed cooperating witnesses.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. This application seeks warrants to search two devices. The first device to be searched, as described in Attachment 1-A is an HTC phone bearing IMEI number 990007191696456 and serial number HT6AD0100385 recovered from RICHARD LUTHMANN on or about December 15, 2017 (the "Luthmann Device"). The second device to be searched, as described in Attachment 2-A, is an iPhone, without a model number, bearing the UDID 05a8ceaebd6863975cd5ebea6d93b5bb21a52044 that was recovered from GEORGE PADULA III on or about December 15, 2017 (the "Padula Device"). The Luthmann Device and the Padula Device are collectively referred to as the "DEVICES."

5. The applied-for warrants would, respectively, authorize the forensic examination of the Luthmann Device for the purpose of identifying electronically stored data particularly described in Attachment 1-B, and the forensic examination of the Padula Device for the purpose of identifying electronically stored data particularly described in Attachment 2-B

PROBABLE CAUSE

6. On or about December 15, 2017, LUTHMANN and PADULA were arrested on an indictment charging them with kidnaping, in violation of 18 U.S.C. § 1201(a)(1), kidnaping conspiracy in violation of 18 U.S.C. § 1201(a), extortionate collection of credit, in violation of

18 U.S.C. § 894(a), extortionate collection of credit conspiracy, in violation of 18 U.S.C. § 894(a), brandishing a firearm during and in relation to those crimes of violence, in violation of 18 U.S.C. § 924(c), wire fraud conspiracy, in violation of 18 U.S.C. § 894(a), money laundering, in violation of 18 U.S.C. § 1957, money laundering conspiracy, in violation of 18 U.S.C. § 1957, and aggravated identity theft, in violation of 18 U.S.C. § 1028A. LUTHMANN was also charged with access device fraud, in violation of 18 U.S.C. § 1029 and an additional count of aggravated identity theft, in violation of 18 U.S.C. § 1028A. A third co-defendant, MICHAEL BECK, was also charged with kidnaping conspiracy in violation of 18 U.S.C. § 1201(a), extortionate collection of credit, in violation of 18 U.S.C. § 894(a), extortionate collection of credit conspiracy, in violation of 18 U.S.C. § 894(a) and brandishing a firearm during and in relation to those crimes of violence, in violation of 18 U.S.C. § 924(c). Based on the facts set forth in this affidavit, there is probable cause to believe that the Luthmann Device and the Padula Device contain evidence of these crimes being committed by these defendants.

7. RICHARD LUTHMANN is the founder of The Luthmann Law Firm PLLC (the "Firm"), the main office of which is located at 1811 Victory Boulevard, Second Floor, Staten Island, New York 10314 (the "Office"). From in or around late Summer 2015 through Spring 2016, LUTHMANN, PADULA and a co-operating witness ("the CW") participated in a fraudulent scrap metal business.[1]

---

[1] The CW has pleaded guilty pursuant to a cooperation agreement to Hobbs Act extortion and wire fraud conspiracy in the hope of gaining leniency at sentencing. The CW has a previous conviction for fraud. His statements have been corroborated by other evidence.

8. The CW has explained that he initially met LUTHMANN four or five years ago and that LUTHMANN represented him in a number of civil suits arising out of a scrap metal business the CW operated. In or around Spring 2015, LUTHMANN introduced the CW to LUTHMANN's friend and former client, PADULA, and LUTHMANN proposed that they all become partners in a fraud based on selling scrap metal to China. LUTHMANN told the CW that PADULA was a valuable person to have involved because PADULA was an associate of a New York-based organized crime family and PADULA's connections to organized crime could be helpful if there was ever a conflict with any of the fraud victims.

9. The CW explained that scrap metal is sold to China in shipping containers. Customers pay based on the weight of the containers. For the fraud LUTHMANN suggested that they fill the containers primarily with cheap "filler" materials, including just enough valuable scrap metal on top and poking through pre-drilled holes on the container to dupe anyone cursorily inspecting the containers. According to the CW, customers would sometimes send a representative to inspect the containers and watch the containers get loaded. The representatives typically would be satisfied by seeking the valuable metal through the holes and were more concerned about being swindled on weight.

10. LUTHMANN created a number of documents for the fraud, including a sheet (the "Review Sheet") he wanted customer representatives to fill out stating they had seen the containers get loaded. The Review Sheet required the signer to include his Driver's License number and to "certify under the penalties of perjury" that the form was correct. LUTHMANN told PADULA and the CW that having the Review Sheet would allow them to claim that any problems with the shipment occurred after the material left the warehouse they were using for the fraud.

11. Throughout the fraud, the CW would communicate with LUTHMANN and PADULA using their cell-phone numbers.

12. According to the CW, LUTHMANN also arranged to have a man he knew ("CS1") be the nominal President of the fraudulent companies, one of which LUTHMANN named Commercial Metals ("Commercial") and one of which he named Omni Metal Company ("Omni"). The fraud was committed primarily through Omni. LUTHMANN told the CW that CS1 is blind and mentally impaired and therefore the perfect front for Omni because he would not be able to identify them if the fraud were detected, and because he could not be sued due to his mental handicap. The address of record for both Commercial and Omni at the time of their corporate filings was the Office. [2]

13. LUTHMANN, PADULA and the CW began the process of helping CS1 open bank accounts for Omni. Several banks refused to open an account for CS1. Ultimately, the primary bank account that was used for Omni was at Israel Discount Bank ("IDB"). LUTHMANN spoke to an acquaintance of his at IDB, where LUTHMANN was also already a client, and arranged for a bank account to be set up for Omni in CS1's name (the "IDB Account"). From in or around November 2015 to December 2015, fraud victims wired hundreds of thousands of dollars in cash to the IDB Account. The CW and another co-

---

[2] CS1 has been meeting with the government and has provided proffer-protected information consistent with the CW. CS1's statements have been corroborated by other evidence. On or about October 11, 2017, the Honorable Nicholas G. Garaufis, United States District Court Judge, issued an order immunizing CS1 for future testimony. CS1 has a sealed conviction from 20 years ago and has advised that he was convicted of assaulting his girlfriend, while he was withdrawing from opiates he had been prescribed in the hospital. He served three days in jail for that incident. CS1 also has an open charge for an assault that allegedly occurred on September 6, 2017.

conspirator then took CS1 to IDB to withdraw over $100,000 in cash over the course of less than two months. IDB bank records and video surveillance footage corroborate this information. Additionally, large sums were wired directly to Luthmann's IOLA account. Over the course of less than two months, nearly $400,000 flowed in and out of the IDB Account.

14. A representative from IDB has confirmed that all documentation regarding the IDB Account was mailed to the Office, including the debit card associated with the IDB Account, which bore the name of Omni and the name of CS1. CS1 confirmed that he never received a debit card from IDB, and the CW stated that he never saw the debit card associated with the IDB Account.

15. On or about December 7, 2016, while the CW was recovering from heart surgery, $10,500 (broken into three separate transactions) was debited from the IDB Account and charged to the Firm, using the debit card associated with the IDB Account. The transactions were processed using a credit card processor at the Office. According to records from Intuit, credit card payments are still being processed from the Office.

16. From in or around Fall 2015 through in or around Spring 2016, LUTHMANN, PADULA and the CW also had fraud victims wire money directly to LUTHMANN's IOLA account, to a Northfield Bank account in CS1's name and to a TD Bank account in CS1's name.

17. After receiving each fraud victim's wire, LUTHMANN, PADULA and the CW would divide the proceeds, often at the Office. They would also sometimes celebrate large transactions at a bar downstairs from the Office and at lunches.

18. An attorney who worked as an independent contractor for the Firm from in or around November 2014 through January 2016 ("CS2") took notes at several meetings related to a scrap metal venture involving Luthmann, Padula, the CW and CS1, which CS2 then placed in

files, though CS2 cannot remember how the files were labeled.[3] CS2 also testified that his timesheets reflected hours billed toward the venture, and that he provided hard copies of his timesheets to LUTHMANN's receptionist, who he understood maintained them. At one point a victim of the scheme called the Office to complain about having been defrauded. LUTHMANN told CS2 to call the victim back, gather information and delay in responding to the victim. LUTHMANN told CS2 to "expect a lot of these calls." Prior to the victim's call, CS2 had been concerned about the venture, but after that interaction he believed it to be a fraud.

19. In or around January 2016, IDB bank contacted CS1, LUTHMANN and others with questions about activity in the IDB Account, including questions about why so much money was being directed to LUTHMANN. In an email, LUTHMANN, using the email address rluthmann@luthmannfirm.com, claimed, for example, that from one $191,000 payment from the IDB Account to the Firm, $173,000 was paid to "cover Omni Metal obligations/expenses including insurance, debt service, materials, etc." No further documentation was provided to IDB to explain this movement of money.

20. Both during and after the fraud, LUTHMANN frequently demanded legal fees from the CW that LUTHMANN said he was owed for work he did for the CW.

---

[3] CS2 was terminated by LUTHMANN in or around January 2016. Prior to CS2's termination, LUTHMANN and CS2 had had a falling out regarding the amount of time CS2 was billing. LUTHMANN and CS2 also had disagreements in Winter and Spring 2016 regarding items CS2 took from the Office. CS2 believed that the venture involving LUTHMANN, PADULA and the CW involved fraud, but he hoped to benefit financially from it, at least by receiving a substantial bonus at the end of 2015, which CS2 did not. CS2 has been voluntarily providing proffer-protected information, and the government is continuing to assess his criminal exposure. CS'2 information has been corroborated by other evidence.

21. In or around January 2016, while the CW was still recovering from heart surgery, PADULA visited him and informed him that LUTHMANN wanted legal fees paid. The CW gave PADULA cash to pay LUTHMANN, but was short by approximately $7,000. PADULA agreed to loan the CW the $7,000.

22. Eventually the CW grew frustrated with sharing fraud proceeds with PADULA, and in or around Summer 2016, the CW began a new fraudulent company with someone else.

23. In or around August 2016, LUTHMANN told the CW that Chinese men had shown up at his office, one with a gun, looking for Omni, because the address for the Office was listed on all of the Omni documents. LUTHMANN said that he had had a private investigator research these men and learned they were members of Chinese organized crime. LUTHMANN and PADULA told the CW that they had to have MICHAEL BECK, an enforcer for the same crime family as PADULA's father and uncle, and one of PADULA's criminal associates, conduct a "sit down" with the Chinese men. At the direction of LUTHMANN and PADULA, the CW paid a total of $23,000 to PADULA for BECK ($3,000 as a show of good faith and then $20,000 for the actual "sit down") with the understanding PADULA and LUTHMANN would each pay $20,000 to BECK as well. The CW understood that BECK and PADULA's uncle had a "sit down" with the Chinese men and resolved the conflict.

24. According to the CW, on or about December 5, 2016, LUTHMANN arranged for the CW to come to the Office under the guise of having the CW sign some legal paperwork and to meet before going out together for the evening, including by sending text messages and making calls from LUTHMANN's cellphone.

25. When the CW arrived at the Office, LUTHMANN was not there. The CW contacted LUTHMANN, who told him to wait inside. While the CW was waiting in the Office,

PADULA and BECK (who Luthmann had previously told the CW was "muscle" for PADULA) entered the Office. BECK pulled out a gun and aimed it at the CW's head and knee. BECK told the CW that the CW owed BECK $10,000 because PADULA had loaned the CW $7,000 and BECK had then purchased that debt and added a $3,000 "vig," or interest payment. Toll records and evidence recovered from the CW's phone show the CW in communication with LUTHMANN before the incident and trying to contact him after the incident. Additionally, the CW has made consensual recordings of LUTHMANN in which LUTHMANN admits luring the CW to the Office knowing that PADULA and BECK intended to speak to him about money, but denies knowing that they had a gun.

26. In or around the next several weeks of December 2016, the CW received calls and text messages from LUTHMANN and PADULA from their cellphones, indicating that PADULA wanted to see the CW. The CW did not contact PADULA.

27. On or about December 28, 2016 and December 29, 2016, the CW and the CW's son received text messages from a phone number they were unfamiliar with. The messages to the CW included the following: (1) "How far would you like this to go? I guess you think you're going to ignore this. No problem. Remember you're taking this to a new level."; (2) "I promise I will see both your sons this week. You must think I'm nothing. You're going to find out real soon how serious I am. I'll give you 10 minutes to get back to me or I'm speaking with your sons this week."; (3) "Ok, all done. You can't steal form me like you steal from all those Chinese people."; and (4) "I'm in red bank you can meet me here or I'll come to your house. Please don't make me come to your house." Red Bank is a town in New Jersey where, according to the CW, he would occasionally meet PADULA to provide PADULA with cash.

28. In or around early 2017, after CS1 was approached by law enforcement, LUTHMANN began refusing to take calls from CS1, and had one of his employees tell CS1 to come pick up his files from the Office.

29. From in or around February 2017 through June 2017, the CW made several consensual recordings of LUTHMANN.

30. On another consensual recording from on or about June 13, 2017, LUTHMANN discussed the December 5, 2016 gunpoint extortion at the Office. In sum and substance, LUTHMANN explained that on December 5, 2016, PADULA and BECK told him to have the CW come to the Office. On the recording LUTHMANN said, "[H]alf hour before you [the CW] were supposed to get there they said get the fuck out and don't tell anybody." LUTHMANN denied knowing PADULA and BECK were going to extort the CW with a firearm but admitted thinking there "was a money issue."

31. Also on the June 13, 2017 recording, LUTHMANN discussed a recent conflict he had had with PADULA and BECK and said he told one or both of them, "Next time you come at me, come heavy or not at all. I got a Glock waiting in my office drawer, and I got a shotgun right behind me, and you won't know the fucking difference when it hits you." In my training and experience, "Glock" and "shotgun" are references to firearms. LUTHMANN's credit card statement also reflects membership fees paid to the National Rifle Association. LUTHMANN does not have a New York State firearms license.

32. LUTHMANN and PADULA both use a service called TrapCall, which in some instances disguises the numbers they are calling or receiving calls from on their phone records. However, an analysis of LUTHMANN'S, PADULA'S and BECK's cellphone records and TrapCall records show calls between and among each of them, including during the time of the

fraud and in or around December 5, 2016, using the cell-phone numbers known to belong to each of them.

33. Based on my training, experience and knowledge of this investigation, I know that information stored on the DEVICES may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

34. Based on my training, experience and knowledge of this investigation, I know that LUTHMANN, PADULA and BECK used cellphones to communicate with each other, and that LUTHMANN and PADULA used cellphones to communicate with the CW.

35. Based on my training, experience and knowledge of this investigation, I know that individuals engaged in fraud and violent crime frequently store their criminal associates' contact information in their cellular telephones.

36. In addition, based on my training and experience, I know that members and associates of organized crime often maintain records, such as the telephone numbers and text messages of their associates and victims, in their cellphones. Those who commit such offenses may also retain evidence of their participation in such crimes on their cellphones through call records, text messages, other messenger applications, emails or photos. Furthermore, I know from my training and experience that cellular telephones maintain call logs that record incoming and outgoing telephone numbers, as well as the date and time of the call. This information is important to identify any telephone communications that relate to important events in this case. Moreover, based upon my training and experience, I know that these call logs, messages, emails and photos will remain on the devices once put on there

unless affirmative steps are taken to delete them or, in the case of call logs, unless subsequent calls are made forcing earlier calls out of the memory.

37. The DEVICES are currently in the lawful possession of the FBI. They came into the FBI's possession after LUTHMANN and PADULA were placed under arrest by the FBI and the DEVICES were seized incident to a lawful arrest. Therefore, although FBI might already have all necessary authority to examine the DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the DEVICES will comply with the Fourth Amendment and other applicable laws.

38. At the time of his arrest LUTHMANN acknowledged that the Luthmann Device was his cellular phone, and while he was being processed, LUTHMANN used the Luthmann Device to call his lawyer whose number he had in the contacts section of the Luthmann Device. Furthermore, the records received from Verizon Wireless listing Luthmann's cellular telephone lists the same IMEI number as belongs to the LUTHMANN Device and lists the same phone number for that device as the CW used to communicate LUTHMANN during and after the fraud.

39. At the time of his arrest, PADULA acknowledged that the Padula Device was his cellular phone, and that morning PADULA was allowed to call his lawyer and mother using the Padula Device. Toll records reflect that at the time PADULA was allowed to call his mother and lawyer from the Padula Device, his mother and lawyer received calls from the same number that the CW used to communicate with PADULA during and after the fraud.

40. The DEVICES are currently in storage at FBI's offices in Kew Gardens, New York. In my training and experience, I know that the DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES first came into the possession of the FBI.

TECHNICAL TERMS

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash

memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

e. IP Address: An IP address is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

42. Based on my training, experience, and research, I know that the DEVICES have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or

suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. *Forensic evidence.* As further described in Attachments B-1 and B-2, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

46. *Manner of execution.* Because this warrant seeks only permission to examine devices that are already in the custody of the FBI, the execution of this warrant does not involve a separate physical intrusion onto a premises. Consequently, I submit there is

reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

47. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Luthmann Device described in Attachment A-1 to seek the items described in Attachment B-1, and probable cause for a search warrant authorizing the examination of the Padula Device described in Attachment A-2 to seek the items described in Attachment B-2.

Respectfully submitted,

Paul Tambrino
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 22, 2018:

S/ Pohorelsky

ATTACHMENT A-1

The property to be searched is an HTC phone bearing IMEI number 990007191696456 and serial number HT6AD0100385 that was recovered from RICHARD LUTHMANN on or about December 15, 2017 (the "Device"). The Device is currently in law enforcement custody in Kew Gardens, New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B-1.

ATTACHMENT B-1

1. All records on the device described in Attachment A-1 that constitute fruits, evidence and instrumentalities of violations of kidnaping, in violation of 18 U.S.C. § 1201(a)(1), kidnaping conspiracy in violation of 18 U.S.C. § 1201(a), extortionate collection of credit, in violation of 18 U.S.C. § 894(a), extortionate collection of credit conspiracy, in violation of 18 U.S.C. § 894(a), brandishing a firearm during and in relation to those crimes of violence, in violation of 18 U.S.C. § 924(c), wire fraud conspiracy, in violation of 18 U.S.C. § 894(a), money laundering, in violation of 18 U.S.C. § 1957, money laundering conspiracy, in violation of 18 U.S.C. § 1957, aggravated identity theft, in violation of 18 U.S.C. § 1028A, and access device fraud, in violation of 18 U.S.C. § 1029, since on or about August 1, 2015, including:

a. All records and information on the Device described in Attachment A-1, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, FaceTime logs, Google Voice calls, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of the above-listed crimes;

b. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. Evidence of the lack of such malicious software;

e. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

g. Evidence of the times the Device was used;

h. Passwords, encryption keys, and other access devices that may be necessary to access the Device; and

i. Contextual information necessary to understand the evidence described in this attachment, all of which constitutes evidence, fruits and instrumentalities of the above-listed crimes;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT A-2

The property to be searched is an iPhone, without a model number, bearing UDID 05a8ceaebd6863975cd5ebea6d93b5bb21a52044 that was recovered from GEORGE PADULA III on or about December 15, 2017 (the "Device"). The Device is currently in law enforcement custody in Kew Gardens, New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B-2.

ATTACHMENT B-2

1. All records on the device described in Attachment A-2 that constitute fruits, evidence and instrumentalities of violations of kidnaping, in violation of 18 U.S.C. § 1201(a)(1), kidnaping conspiracy in violation of 18 U.S.C. § 1201(a), extortionate collection of credit, in violation of 18 U.S.C. § 894(a), extortionate collection of credit conspiracy, in violation of 18 U.S.C. § 894(a), brandishing a firearm during and in relation to those crimes of violence, in violation of 18 U.S.C. § 924(c), wire fraud conspiracy, in violation of 18 U.S.C. § 894(a), money laundering, in violation of 18 U.S.C. § 1957, money laundering conspiracy, in violation of 18 U.S.C. § 1957, aggravated identity theft, in violation of 18 U.S.C. § 1028A, and access device fraud, in violation of 18 U.S.C. § 1029, since on or about August 1, 2015, including:

a. All records and information on the Device described in Attachment A-2, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, FaceTime logs, Google Voice calls, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of the above-listed crimes;

b. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. Evidence of the lack of such malicious software;

e. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;

f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;

g. Evidence of the times the Device was used;

h. Passwords, encryption keys, and other access devices that may be necessary to access the Device; and

i. Contextual information necessary to understand the evidence described in this attachment, all of which constitutes evidence, fruits and instrumentalities of the above-listed crimes.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.